REMARKS

Applicants appreciate the Examiner's thorough examination of the subject application and request reconsideration of the subject application based on the foregoing amendments and the following remarks.

Claims 1-6 and 8-22 are pending in the subject application. Claim 7 was previously canceled.

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103.

Claim 2 was objected to because of identified informalities. As it appears that the objection is directed to the legend, Applicants understand the Examiner's objection to be an indication that the amended claim was not entered into the record and that the amended claim 2 should be represented herein with a proper legend. Thus, claim 2 was represented in amended form herein with the proper legend.

Claims 1, 17 and 18 were amended for clarity and to more distinctly claim Applicants' invention.

The amendments to the claims are supported by the originally filed disclosure.

35 U.S.C. §103 REJECTIONS

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103 as being unpatentable over the cited prior art for the reasons provided on pages 2-9 of the above referenced Office Action. Applicants respectfully traverse as discussed below. Because claim(s) was/were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the cited reference. The following addresses the specific rejections provided in the above-referenced Office Action.

CLAIMS 1-14, 17-22

Claims 1-6, 8-14 and 17-22 stand rejected as being unpatentable over Burns et al. [USP 6,405,315; "Burns"] in view of Flyntz [US Patent Application Publication 2002/0147924] for the reasons provided on pages 3-8 of the above-identified Office Action. Applicants respectfully traverse.

As previously indicted by Applicants, it appears that there may be some confusion as to a user of a network computer and the term "network client" in Burns. As described in Burns, a network client is the computer that is attached to the network (see col. 1, l. 30-35 of Burns) Burns also provides that a network client corresponds to the components of the file system that request data from the devices (see col. 5, l. 25-35 of Burns). Thus, nowhere in Burns is the term "network client" equated with the user of a computer.

While a user can provide inputs or instructions to a computer, the inputs or instructions are carried out by the computer operating system and applications programs and any instructions or criteria embedded in these programs. It is specifically described in Burns, that the decryption and encryption functions are only carried out by the network clients, which makes it abundantly clear that the user is not a network client as that term is used in Burns. Therefore, Applicants again submit that Burns does not describe, teach or suggest the claimed invention to the extent that the rejections are based on the incorrect assumption that a network client equates to a user. Such an assertion is completely inconsistent with the description in Burns.

The electronic network device of claim 1, includes (*inter alia*)

(a) a setting section for setting a security level for the data to be transmitted, wherein the security level is set in the setting section responsive to an input from a user of the electronic device, where the set security level being selected by the user is selected from a plurality of identified security levels;

(b) the electronic device, at least one of the plurality of storing means, and at least one of the plurality of external devices each have a security function and another security level associated with the set security level;

(c) a search means for searching the plurality of storing means and for searching the plurality of external devices to identify one or more given storing means or one or more given external devices whose security level corresponds to the security level set in the setting section;

(d) a selecting means for providing results of the searching to the user and for providing an output, the output corresponding to a selected one of the identified one or more given storing means or the identified one or more given external device whose security level corresponds to the security level set in the setting section, the selected one being selected by the user from the provided search results; and

(e) the electronic device transmits the data to the selected one of the given storage means or the given external device responsive to said output from the selecting means.

In other words in the electronic network device of claim 1, (1) the user sets a security level from a plurality of such security levels for the data to be transmitted, (2) a search is made to identify those storing means and external devices that whose security level corresponds to the security level set in the setting section, (3) the results of the searching are provided to the user who selects one of the storing means and external devices that were identified in (2) and after the user selects the one, the electronic network device transmits the data to the selected one. Thus, the electronic device of claim 1 is configured and arranged so that the user provides inputs at different times which inputs are utilized to control the electronic network device.

In contrast to the present invention, Burns describes a decentralized remotely encrypted file system, that includes a plurality of storage devices which serve as a repository of the system's data. As also described in Burns, the data is encrypted by the network clients before it is sent to a storage device and the data read from the storage device is decrypted by the network client. In other words, and as previously indicated by Applicants (and admitted by the Examiner), the storage devices in Burns all have the same security level.

As to the assertion that Burns describes in col. 9, ll. 1-25 a setting section for setting a security level and that the set security level is selected by the user from a plurality of security levels. Applicants respectively disagree. As previously indicated by Applicants, this discussion in Burns (which starts in col. 8) describes the well known process for locking for cache consistency. This process does not involve setting a security level or selecting a security level from a plurality of available levels. The process described in Burns relates to the process undertaken by the operating system to prevent a user from writing to a file while another user also is writing to the same file. Similarly the process is provided to prevent a user from reading or writing when another has accessed the file for a read/write. The methodology described in Burns involves the use of a lock manager that locks (*i.e.*, spin locks) access to the file until the present operation is completed.

In sum, the discussion in Burns cited in support for the asserted structure or function as nothing to do with setting security levels.

Flyntz teaches that the computer operates in default to the security subsystem having the lowest security level (no security) and that the other security subsystem(s) requires the insertion of a card that is read by the computer to determine what access level is being sought. To maintain security, Flyntz teaches that in the case where the local system is to be operated using a security subsystem of a higher level, power is only provided to security subsystem being operated. In other words, if the computer is using another security sub-system, the power is terminated to the another security sub-system. Thus, while Flyntz might teach that a local system or computer may include a plurality of security sub-systems, security access to the individual subsystems is controlled by not providing power to the sub-system(s) not being used.

As to the assertions that Burns searches for a storage device having the security level set in a setting section, the discussion in Burns regarding Fig. 7 describes the function directed to locating the specified object and returns the object's attributes and the object's directory if found (see col. 10, l. 20-40). Basically, the process shown in Fig. 7 and described in Burns, is the lookup operation that is used to implement a virtual file system.

This does not describe the search section as set forth in claim 1, where a search is made of all of the external devices and storage means connected to a network to identify the one or more external devices or storage means whose security level corresponds to the security level set in the setting section. As also described in the subject application, if the search does not reveal any such storage means or external devices, the user can alter the search parameters and perform another search.

If such external devices or storage means are identified, as set forth in claim 1, the results of the search are provided to the user and the user selects from the search results a specific one of the identified external device(s) or storage means having a corresponding security level and an output of the selected one is made. Thereafter, the electronic device transmits the data to the specific one of the identified external devices or storage means based on this output.

Such a process and related structure is not described anywhere in Burns or Flyntz. This is not surprising as the network client is the functionality carrying out the described functions without the need for evaluation of input from the user.

As to claims 2-3, 6 and 8-13, each of these claims depends (directly or ultimately) from claim 1. Thus, each of claims 2-3, 6 and 8-13 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 2-3, 6 and 8-13 are not separately patentable from the combination of Burns and Miyazaki.

As to claim 17, Applicants respectfully submit that the above remarks regarding claim 1, apply to distinguish the data receiver search system of claim 17 from the combination of Burns and Miyazaki. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 17 from the combination of Burns and Miyazaki.

As to claim 18, Applicants respectfully submit that the above remarks regarding claim 1 apply to distinguish the data receiver search method of claim 18 from the combination of Burns and Miyazaki. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 18 from the combination of Burns and Miyazaki.

As to claims 19-22, each of these claims depends (directly or ultimately) from claim 18. Thus, each of claims 19-22 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 19-22 are not separately patentable from the combination of Burns and Miyazaki.

It is respectfully submitted that claims 1-6, 8-14 and 17-22 are patentable over the cited reference(s) for the foregoing reasons.

CLAIMS 15-16

Claims 15 and 16 stand rejected as being unpatentable over Burns et al. [USP 6,405,315; "Burns"] in view of in view of Flyntz [US Patent Application Publication 2002/0147924] and further in view of Tomat [USP 6,459,499]. Applicants respectfully traverse as discussed below. Because claims were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the cited reference.

Each of claims 15-16 depends (directly or ultimately) from claim 1. Thus, each of claims 15 and 16 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 15-16 are not separately patentable from the combination of Burns, Miyazaki and Tomat.

It is respectfully submitted that claims 15 and 16 are patentable over the cited reference(s) for the foregoing reasons.

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F. 2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). As provided above,

the references cited, alone or in combination, include no such teaching, suggestion or motivation.

Furthermore, a prior art reference can be combined or modified to reject claims as obvious as long as there is a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 19866). Additionally, it also has been held that if the proposed modification or combination would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. Further, and as provided in MPEP-2143, the teaching or suggestion to make the claimed combination and the reasonable suggestion of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). As can be seen from the forgoing discussion regarding the disclosures of the cited references, there is no reasonable expectation of success provided in the references that the suggested modification would be reasonably successful. Also, it is clear from the foregoing discussion that the modification suggested by the Examiner would change the principle of operation of the system and methodology described in Burns.

It is respectfully submitted that for the foregoing reasons, claims 1-6 and 8-22 are patentable over the cited reference(s) and thus, satisfy the requirements of 35 U.S.C. §103. Therefore, these claims are allowable.

It is respectfully submitted that the subject application is in a condition for allowance. Early and favorable action is requested.

Applicants believe that additional fees are not required for consideration of the within Response. However, if for any reason a fee is required, a fee paid is inadequate or credit is owed

for any excess fee paid, the Commissioner is hereby authorized and requested to charge Deposit

Account No. **04-1105**.

Respectfully submitted,

Edwards Angell Palmer & Dodge, LLP

/ William J. Daley, Jr. /

Date: August 26, 2008   By: _____

William J. Daley, Jr.
(Reg. No. 35,487)
P.O. Box 55874
Boston, MA 02205
(617) 239-0100

Customer No. 21,874

Bos2_682545